EIN KOMBINATORISCHER BEWEIS EINES SATZES VON FERMAT

VON

AXEL THUE

(Videnskabs-Selskabets Skrifter. I. Math.-Naturv. Klasse 1910. No. 3)

UDGIVET FOR FRIDTJOF NANSENS FOND

CHRISTIANIA
IN KOMMISSION BEI JACOB DYBWAD
1910

Fremlagt i den math.-naturv. Klasses Møde 19. November 1909.

A. W. BRØGGERS BOGTRYKKERI.

Es seien a und n zwei beliebige ganze positive Zahlen. Ferner seien

$$G_1 \; G_2 \; G_3 \cdots\cdots G_a$$

a verschiedene Sorten von Gegenständen oder Zeichen und

$$P_1 \; P_2 \; P_3 \cdots\cdots P_n$$

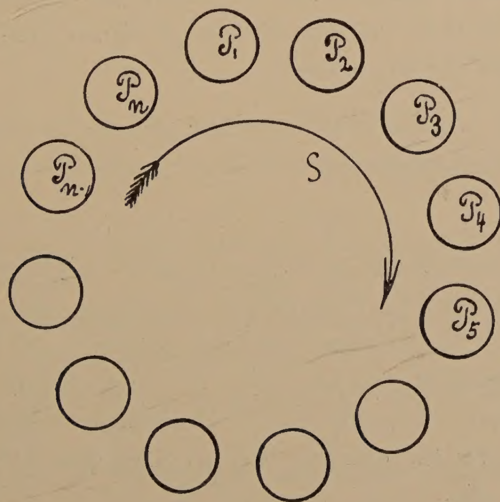
n verschiedene Plätze.

Auf jeden der n Plätze P können wir nun einen Gegenstand von einer beliebigen der a Sorten anbringen.

Sagen wir nun, dass zwei solche Placierungen von n Gegenständen G auf die n Plätze dann und nur dann einander gleich seien, wenn auf jeden beliebigen der n Plätze bei beiden Placierungen beziehungsweise zwei Gegenstände G derselben Sorte angebracht sind, dann giebt es im ganzen

$$a^n$$

verschiedene solche Placierungen.



Von einer beliebig gegebenen Placierung A der oben erwähnten Art können wir eine neue B erhalten, indem wir für alle die betreffenden

Werte von x den Gegenstand, der durch die Placierung A auf den Platz P_x placiert ist, auf den neuen Platz P_y, wo $y \equiv x + 1 \pmod{n}$, stellen.

Wir wollen sagen, dass die Placierung B aus der Placierung A durch die Operation S erhalten ist.

Wendet man die Operation S n Male auf eine beliebige unserer Placierungen an, so wird die erhaltene Placierung der ersten gleich.

Satz 1.

Bedeutet U_a^n die Anzahl sämtlicher derjenigen von unseren a^n Placierungen, wovon jede so beschaffen ist, dass sie nicht nach weniger als n Anwendungen der Operation S in sich selber übergeht, dann muss U_a^n immer durch n teilbar sein.

Aus einer willkürlichen Placierung T_1 von den U_a^n Placierungen können wir nämlich $n - 1$ neue Placierungen $T_2\ T_3 \cdots\cdots T_n$ durch successive Anwendungen der Operation S bilden, indem T_{x+1} von T_x durch eine einzige Anwendung der Operation S gebildet ist.

Je zwei der n Placierungen $T_1\ T_2 \cdots\cdots T_n$, die nach der Voraussetzung sämtlich verschieden sind, können durch wiederholte Anwendung der Operation S in einander überführt werden.

Anwendet man die Operation S auf eine beliebige der n Placierungen T eine beliebige Anzahl Male, so erhält man wieder eine der Placierungen T.

Jede der Placierungen T wird eine der genannten U_a^n Placierungen.

Es sei nun W_1 eine von T_1 verschiedene der U_a^n Placierungen und $W_2\ W_3 \cdots\cdots W_n$ alle die von W_1 durch die Operation S successiv gebildeten von einander und von W_1 verschiedenen Placierungen.

Ist dann eine der Placierungen

$$W_1\ W_2 \cdots\cdots W_n$$

mit einer der Placierungen

$$T_1\ T_2 \cdots\cdots T_n$$

identisch, dann enthalten beide Reihen dieselben n Placierungen.

Für jede von den U_a^n Placierungen erhält man also auf diese Weise eine Reihe von n Placierungen unter den genannten U_a^n Placierungen.

Da nun sämtliche verschiedenen von diesen Reihen von n verschiedenen Placierungen im ganzen alle U_a^n Placierungen enthalten müssen und jede Placierung nur ein einziges Mal, so muss also U_a^n, wie behauptet, durch n teilbar sein.

Ist z. B. n eine Primzahl, bekommt man

$$U_a^n = a^n - a$$

Giebt es nämlich eine Placierung, die durch eine einzige Anwendung der Operation S in sich selber übergeht, so müssen hier auf allen n Plätzen Gegenstände derselben Sorte stehen.

Es giebt folglich im ganzen a solche Placierungen.

Wir brauchen folglich, nach unserem Satze, nur zu zeigen, dass wenn eine beliebige Placierung R von den restierenden

$$a^n - a$$

Placierungen durch r Anwendungen der Operationen S in sich selber übergeht, dann kann r nicht kleiner als n sein.

Wenn nämlich das der Fall wäre, müsste auch die kleinste positive Zahl r_0, für welche R nach r_0 Anwendungen der Operationen S in sich selber überging, kleiner als n sein.

Wir bekämen dann in ganzen positiven Zahlen h und k:

$$n = r_0 h + k$$

wo

$$0 < k < r_0$$

indem $r_0 > 1$ ist. Aber wenn $k = n - r_0 h$, ginge R folglich auch nach k Anwendungen der Operationen S in sich selber über, was nach unserer Voraussetzung über die Zahl r_0 unmöglich ist.

Ist n eine Primzahl, muss

$$a^n - a$$

folglich durch n teilbar sein.

Dieser Fermat'sche Satz ist somit bewiesen.

Indem wir nun U_a^n für jede beliebige ganze positive Zahl bestimmen wollen, werden wir dadurch auch eine Erweiterung des Fermat'schen Satzes herleiten.

Man ersieht aus dem obenstehenden Raisonnement gleich ein, dass wenn eine von unseren a_n Placierungen nach δ, wo $\delta > 0$, aber nicht nach weniger als δ Anwendungen der Operationen S in sich selber übergeht, dann muss δ ein Divisor von n sein.

Ferner sieht man auch ein, dass die Anzahl aller solchen Placierungen gleich U_a^δ sein muss.

Da nun jede der a^n Placierungen nach n oder nach weniger Anwendungen der Operationen S in sich selber übergeht, so kann man für jede beliebige Placierung Q, der a^n Placierungen immer einen solchen Divisor δ von n, wo 1 und n als Divisoren betrachtet sind, finden, dass Q nach

δ aber nicht nach weniger als δ Anwendungen der Operationen S in sich selber übergeht.

Wir erhalten auf diese Weise die a^n Placierungen in ebenso viele Klassen geteilt, wie Divisoren δ von n existieren.

Wir bekommen somit folgendes Resultat:

Satz 2.

$$a^n = U_a^\alpha + U_a^\beta + \cdots\cdots + U_a^\gamma \quad \ldots\ldots (1)$$

wo $\alpha, \beta, \cdots\cdots, \gamma$ *sämtliche Divisoren von* n *sind.*

Bezeichnen $p, q, \cdots\cdots, r$ sämtliche verschiedene Primzahlfaktoren von n, so erhält man nach (1)

$$U_a^n = A_1 a^{p^{m_1} q^{s_1} \cdots\cdots r^{t_1}} + \cdots\cdots + A_v a^{p^{m_v} q^{s_v} \cdots\cdots r^{t_v}} + B U_a^1 \quad \ldots\ldots (2)$$

wo die Grössen $m, s, \cdots\cdot,$ und t ganze nicht negative Zahlen und die Grössen A und die Grössen B ganze positive oder negative Zahlen sind.

Bedeutet aber ferner $\varphi(n)$ die Anzahl jener der Zahlen

$$1, 2, 3, \cdots\cdot, n$$

die relative Primzahlen gegen n sind, so wird wie bekannt:

$$n = \varphi(\alpha) + \varphi(\beta) + \cdots\cdot + \varphi(\gamma) \quad \ldots\ldots (3)$$

Da die Gleichungen (1) und (3) einander ähnlich sind, bekommen wir folglich:

$$\varphi(n) = A_1 p^{m_1} q^{s_1} \cdots\cdot r^{t_1} + \cdots\cdot + A_v p^{m_v} q^{s_v} \cdots\cdot r^{t_v} + B\varphi(1) \quad \ldots (4)$$

Nun ist aber:

$$\varphi(n) = n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right) \cdots\cdot \left(1 - \frac{1}{r}\right) \quad \text{oder}$$

$$\varphi(n) = n\left[\frac{(-1)^{\theta_0}}{D_0} + \frac{(-1)^{\theta_1}}{D_1} + \cdots\cdot + \frac{(-1)^{\theta_k}}{D_k}\right] \quad \ldots\ldots (5)$$

wo D_0, $D_1, \cdots\cdot, D_k$ beziehungsweise sämtliche Divisoren von dem Produkte $p, q \cdots\cdot r$ bedeuten, während θ_x für jeden betreffenden Wert von x die Anzahl der Primzahlfaktoren von D_x angiebt.

Ist $D_y = 1$, so wird $\theta_y = 0$.

Durch Vergleichung von (4) und (5) erhalten wir die Grössen A, B, m, s und t.

Man bekommt folglich nach (2), indem wir bemerken, dass

$$U_a^1 = a = a^1, \quad \varphi(1) = 1$$

dass:

$$U_a^n = (-1)^{\theta_0} a^{\frac{n}{D_0}} + (-1)^{\theta_1} a^{\frac{n}{D_1}} + \cdots\cdot + (-1)^{\theta_k} a^{\frac{n}{D_k}} \quad \ldots (6)$$

Wir haben also folgenden Satz gewonnen.

Satz 3.

Bedeuten a und n zwei beliebige ganze positive Zahlen und $p, q, \cdots, r$ die sämtlichen in n aufgehenden von einander verschiedenen Primzahlen und ferner $D_0, D_1, D_2 \cdots, D_k$ die sämtlichen verschiedenen Divisoren von dem Produkte $p\, q \cdots r$, während θ_x für jeden der betreffenden Werte von x die Anzahl der Primzahlfaktoren von D_x angiebt, dann wird die ganze Zahl

$$-(1)^{\theta_0} a^{\frac{n}{D_0}} + (-1)^{\theta_1} a^{\frac{n}{D_1}} + \cdots + (-1)^{\theta_k} a^{\frac{n}{D_k}}$$

immer durch n teilbar sein.

Aus diesem Satze können wir leicht die Euler'sche Erweiterung des Fermatschen Satzes erkennen. Wir wollen doch darauf verzichten.

Wir haben wenn $D_0 = 1$ und $\theta_0 = 0$ also gefunden, dass

$$\left[a^n + (-1)^{\theta_1} a^{\frac{n}{D_1}} + (-1)^{\theta_2} a^{\frac{n}{D_2}} + \cdots + (-1)^{\theta_k} a^{\frac{n}{D_k}}\right] : 1$$

durch n teilbar sein muss.

Ersetzt man hier das Operationszeichen : durch das Operationszeichen — und das Operationszeichen $+(-1)^{\theta}$, welches $+$ oder $-$ bedeuten kann, durch das Operationszeichen . oder :, je nachdem $+(-1)^{\theta}$ das Zeichen $+$ oder $-$ bedeutet, so erhält man den Ausdruck

$$a^n \cdot a^{(-1)^{\theta_1} \frac{n}{D_1}} \cdot a^{(-1)^{\theta_2} \frac{n}{D_2}} \cdots a^{(-1)^{\theta_k} \frac{n}{D_k}} - 1 =$$

$$= a^n \left[1 + \frac{(-1)^{\theta_1}}{D_1} + \frac{(-1)^{\theta_2}}{D_2} + \cdots + \frac{(-1)^{\theta_k}}{D_k}\right] - 1 = a^{\varphi(n)} - 1$$

welcher Ausdruck nach dem Euler'schen Satze auch durch n teilbar ist.

Die obenstehenden Betrachtungen können verallgemeinert werden.

Lian, d. 17. November 1909.

Gedruckt am 5. November 1910.